THABACHWEU LOCAL MUNICIPALITY

User Password

Policy

The Thabachweu Local Municipality policies are statements of principles and practices dealing with the on-going management and administration of the Municipality's IT assets. These policies act as a guiding frame of reference for how the Municipality deals with everything from its day- to-day IT operational and support procedures to comply with security regulations and codes of practice. This "statement of purpose" will guide the actions to be taken to achieve that purpose.

Thabachweu Local Municipality

Table of Contents

1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Municipality's entire corporate network. As such, all the Thabachweu Local Municipality employees, business partners and services providers are therefore responsible for taking the appropriate steps around password security outlined in this document.

2. Purpose

The purpose of the Municipality's password policy is to define a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

This policy governs everyone who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any of the Municipality's facilities, has access to the Municipality's network, or stores information on the Municipality's infrastructure

3. Scope

3.1. Guidelines

Passwords are used for various purposes at the Municipality. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have support for one-time tokens such as dynamic passwords which are only used once therefore everyone must be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Thabachweu ", "municipality", "myname" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, QWERTY, zyxwvuts, 123321, password, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Strong passwords have the following characteristics:
    - Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g., 0-9,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

- Passwords should never be written down or stored on-line.
- Create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

3.2. Password Protection

- All the Municipality's passwords shall be treated as sensitive and confidential.
- Do not use the same password for internal and external (Eg. personal e-mail account and your user account, etc.). Where possible, use different strong passwords for the various systems accessed.
- Do not reveal your passwords with anyone, including administrative and support staff, assistants or secretaries.
- If someone demands a password, refer them to this policy and report the incident to the Municipality's Security Officer.
- Do not use the "Remember Password" feature of applications (e.g., Internet Explorer or Microsoft Outlook).
- Never write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- Change passwords at least once every 30-40 days (except system-level passwords which must be changed every 60-90 days).
- If an account or password is suspected to have been compromised, report the incident immediately to the Municipality's Security Officer.
- Password cracking or guessing tools and utilities may only be used for testing security under the supervision and guidance of the Municipality's Security Officer.

3.3. Domain Password

The "Default domain policy" on the Microsoft Active Directory will govern the following password characteristics:

- Enforce Password History 12 Passwords
- Maximum password age 42 days
- Minimum password age 1 day
- Minimum password length 8 Characters

- Password Complexity Enabled
- Account Lockout Duration 30 Minutes
- Account Lockout Threshold 5 invalid logon attempts
- Reset account lockout counter After 30 minutes

Password protected screen savers should be enabled and should protect the computer within 15 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active.

Users must be educated to lock their computers when they are not in the office.

4. Corrective actions for non-policy compliance

- Failure to comply with the guidelines stipulated in the Municipality's policies will result in the following corrective or disciplinary procedures.
- The decisive action that will be taken against the employee is dependent on the severity level and the level of the security risk.
- Warning from Management
    - The employee receives a warning from their manager that they were in violation of policy.
- Written Warning in Personnel File
    - The employee is reprimanded, and official notice is put in their personnel file. This may have negative consequences during future performance reviews or promotion considerations.
- Revoking Privileges
    - Access to certain resources, such as internet or email, can be revoked for a limited period providing that this action does not have a negative impact on the employee's job functions.
- Training
    - Adequate training to create awareness and guidance on policy compliance.
- Disciplinary action will be determined in compliance to Schedule 8 of the Labour Relations Act 66 of 1995 or other related Public Service Regulations.

5. Glossary and Abbreviations

Please refer to the Thabachweu Glossary and abbreviations guide.

Version Control

Version	State/Change	Author	Date
1.0	Original	Sbusiso Langa	
1.1	Changes	Sbusiso Langa	

Author

Name	Designation	Signature	Contact
Sbusiso Langa	Security Officer		+27 13 235 7367

Review

Name	Designation	signature	Date

Approval

Name	**Designation**	**Signature**	**Date**